COMMUNICATION
NAVIGATION
SURVEILLANCE
Integrated SECURITY SESSION

Marie Stella, CISSP

Marie.stella@faa.gov

NASA I-CNS Conference

April 30, 2002

AGENDA

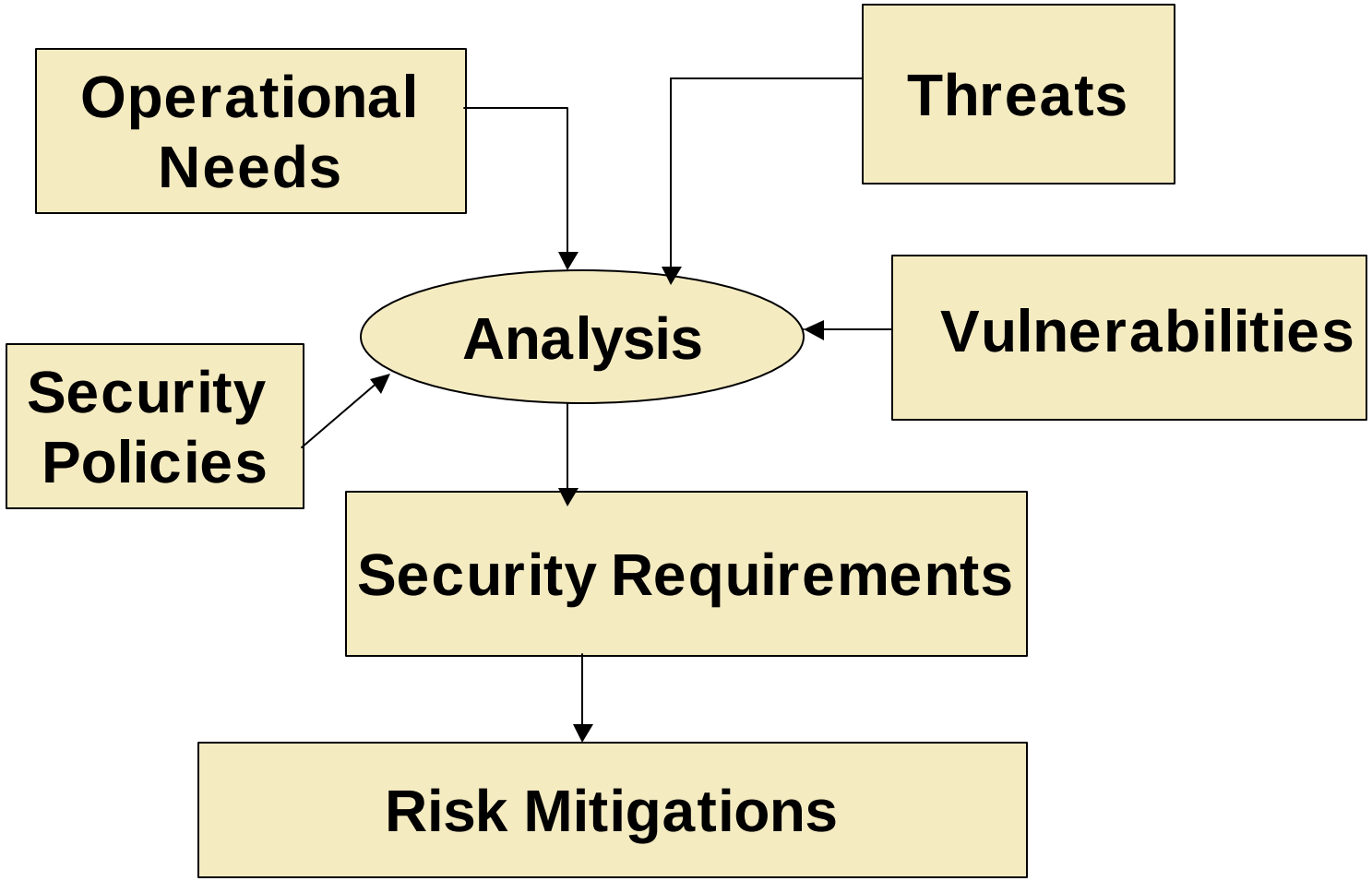
FAA Perspective on Aviation Security

- Generic security requirements analysis
- Application in National Air Space (NAS)
- Current CNS Systems in terms of security
- Security Challenges for the Evolving NAS

Security Enhancements for the NAS via:

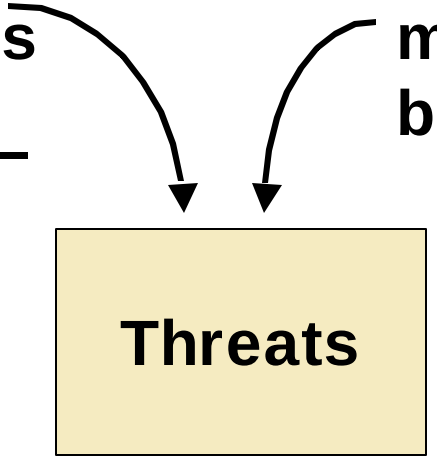
- VHF Data Link for Security Applications
- Front End Security Architecture
- Multi-Center Traffic Management Advisor
- Broadband Satellite Communication Services
- Neural Networks/ Optimize Runway Safety Logic
- Security Considerations for the e-enabled Aircraft

Generic Methodology



Generic Methodology con't.

- Enterprise Security Policies
- Threat Agents – Who and why?



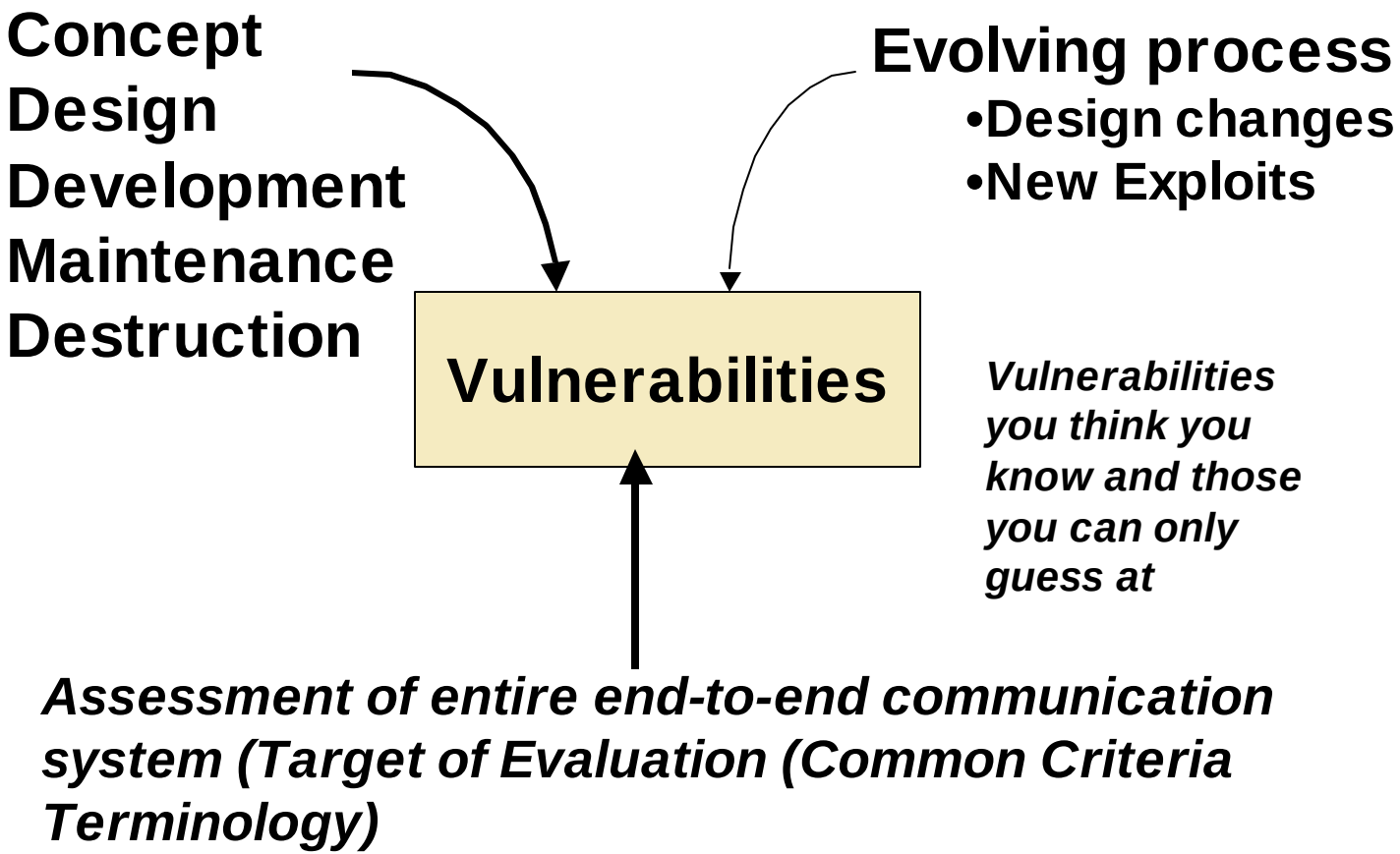
What threat mechanisms will be used
- Physical
- Cyber
  - How
  - When
  - Where

Consequence

Enemies you think you know and those you can only guess at

This brief focuses on Information Security

Generic Methodology con't



Generic Methodology con't

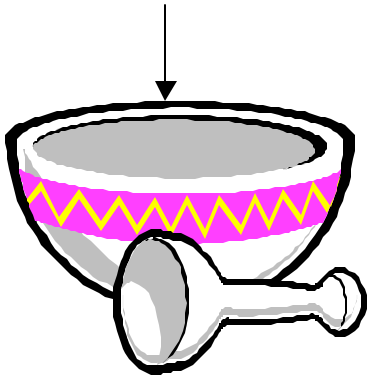
Mission

Operational needs

Vulnerabilities

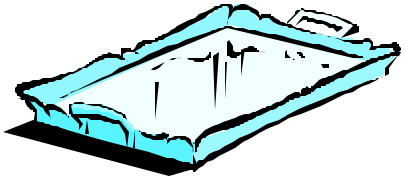
Benefits Costs

Consequences



Mitigation Recipe

Acceptable Risk



Outcome

Generic Methodology con't

Security Requirements

"Every System" Baseline

- OS Patches
- Antivirus SW
- Access control methods
- System Partitioning
- Accountability
- System administration
- Software development, Installation, CM….
- ….

Enterprise/ System Specific

NOT solution phase

Requirement Application in NAS

Enterprise Specific (NAS assumptions and constraints)

- **NAS Security Policy**
  - C2 – (COTS based, no insider threat, no complex attacks
- **NAS Environment**
  - Safety risks mitigated by situational awareness
  - Driven by high availability and high Integrity
  - Primarily Internal Maintenance function
  - Embedded legacy systems
  - Safety, Regulation, acquisitions - long lead times
  - Migration to COTS type systems
  - Testing of all system changes – lead times
- **NAS Culture**
  - (Controller-Pilot) Open communications, trust based
  - Hero Culture
  - Stove-piped organizations-trusted employees
  - Migration to collaborative environment

State of the NAS

Complex, separate systems

→ ***More tightly integrated systems (FREE FLIGHT)***

Legacy systems, obscure protocols

→ ***COTS, TCP/IP, mobile code environment***

Dedicated , leased facilities, closed environment

→ ***Shared services/networks both within and between facilities/partners***

Analog systems – air-to-ground, ground-to-ground

→ ***Digital, integrated v/d services, new technologies***

ATS Voice Communications to the Cockpit

→ ***Voice and Data***

Unchallenged operation – (phantom pilot/controller…

→ ***Fast changing threats and vulnerabilities***

Stable Technology

→ ***Major technology changes yearly***

Security Concerns

What new security requirements are introduced into the NAS by:

- **technology changes,**
- **new system interface**
- **operation changes**
- **National Security needs**

How can we implement these requirements so they are transparent (from a human factors perspective), maintain NAS performance, maintain publics confidence in the NAS?

Further Study

WHAT: Is Authentication needed and where?

HOW: Does the solution address design,implementation, management and recovery from compromise?

WHAT: Is confidentiality needed?

HOW: If so, what is the best methodology and technology?

WHAT: How should National Preparedness requirements be addressed?

HOW: Do we have mechanism, redundancy and alternate technologies to isolate, recover, maintain the NAS?

Challenge for Solution Providers

1) What problem does it solve?
2) How well does it solve the problem?
3) What new problems does it add?
4) What are the economic and social costs?
5) Given the above, is it worth the costs?

Bruce Schneier, Chief Technical Officer

Counterpane Internet Security, Inc.